gartner identity and access management

Gartner Identity and Access Management: Navigating the Future of Secure Access

gartner identity and access management is a phrase that resonates deeply within the cybersecurity and IT management communities. As organizations increasingly rely on digital ecosystems, the demand for robust identity and access management (IAM) solutions has never been higher. Gartner, a leading research and advisory company, offers critical insights and analysis that help businesses understand the evolving landscape of IAM technologies. In this article, we'll explore what Gartner identity and access management entails, why it matters, and how organizations can leverage Gartner’s research to implement effective IAM strategies that safeguard their digital environments while enhancing user experience.

Understanding Gartner Identity and Access Management

At its core, Gartner identity and access management refers to the comprehensive research, evaluations, and frameworks provided by Gartner to help organizations select and implement IAM solutions. Gartner’s analysis covers a wide range of IAM components, including authentication, authorization, user provisioning, governance, and access controls. Their research often culminates in tools like the Magic Quadrant, which evaluates vendors based on their completeness of vision and ability to execute.

What Makes Gartner’s IAM Research Influential?

Gartner’s reputation in the IT industry stems from its rigorous methodology and unbiased approach. When it comes to IAM, Gartner analyzes market trends, emerging technologies, and vendor capabilities, offering organizations a roadmap to navigate the complex IAM ecosystem. This helps decision-makers:

- Understand the strengths and weaknesses of leading IAM vendors
- Stay updated on emerging trends such as Zero Trust and passwordless authentication
- Align IAM strategies with business objectives and compliance requirements

By consulting Gartner’s identity and access management reports, companies gain clarity on which solutions can best support their security posture and scalability needs.

Core Components of Identity and Access Management

To appreciate Gartner’s role in IAM, it’s important to understand the fundamental elements that make up identity and access management systems.

User Authentication and Authorization

Authentication verifies who the user is, often through passwords, biometrics, or multi-factor authentication (MFA). Authorization determines what resources a user can access once authenticated. Gartner highlights the growing importance of beyond-password methods, such as biometric scans and behavioral analytics, to strengthen authentication.

User Provisioning and Lifecycle Management

IAM solutions automate the onboarding and offboarding of users, ensuring that access permissions are granted and revoked appropriately. Gartner emphasizes the need for integration with HR systems and cloud platforms to streamline these processes and reduce security risks tied to orphaned accounts.

Access Governance and Compliance

Monitoring and auditing access rights is crucial for maintaining regulatory compliance and minimizing insider threats. Gartner’s research underscores the value of IAM tools that provide detailed reporting, access reviews, and policy enforcement to meet standards like GDPR, HIPAA, and SOX.

Emerging Trends in Gartner Identity and Access Management

The IAM landscape is rapidly evolving, and Gartner’s insights shed light on key trends shaping the future of identity security.

Zero Trust Security Model

Zero Trust is a paradigm shift that assumes no user or device is inherently trustworthy. Gartner advocates for IAM strategies that support Zero Trust by continuously verifying identities and enforcing least privilege access. This approach reduces the attack surface and limits lateral movement within networks.

Passwordless Authentication

Passwords remain a major vulnerability in cybersecurity. Gartner’s analysis points to a significant move towards passwordless authentication methods, such as biometrics, hardware tokens, and cryptographic keys. These innovations enhance security and improve user convenience.

Cloud and Hybrid IAM Solutions

With cloud adoption accelerating, Gartner highlights the importance of IAM solutions that seamlessly integrate with both on-premises and cloud environments. Hybrid IAM platforms enable organizations to manage identities across diverse infrastructures without compromising security or user experience.

How to Leverage Gartner’s IAM Insights for Your Organization

While Gartner provides extensive research, turning these insights into actionable strategies requires thoughtful planning.

Assess Your Current IAM Posture

Begin by evaluating your existing identity and access controls. Identify gaps in authentication strength, provisioning efficiency, and governance. Use Gartner’s frameworks to benchmark your capabilities against industry standards.

Align IAM with Business Goals

A successful IAM strategy supports business agility and digital transformation initiatives. Gartner advises aligning IAM investments with objectives such as improving customer experience, enabling remote work, and ensuring compliance.

Choose the Right Vendors

Consulting Gartner’s Magic Quadrant and Critical Capabilities reports can guide vendor selection. Consider factors like scalability, ease of integration, support for emerging technologies, and vendor roadmap alignment with your future needs.

Implement Incrementally and Monitor Continuously

IAM deployment should be phased, starting with high-risk areas or business-critical applications. Gartner stresses continuous monitoring and adaptation, as threats and technologies evolve rapidly.

Challenges in Implementing Gartner-Recommended IAM Solutions

Even with Gartner’s guidance, organizations face common hurdles in IAM adoption.

Complexity of Integration

Integrating IAM tools with diverse legacy systems, cloud platforms, and third-party applications can be complex. Gartner recommends prioritizing solutions with robust APIs and pre-built connectors to ease integration efforts.

User Adoption and Experience

Security measures that frustrate users may lead to workarounds, undermining IAM effectiveness. Gartner highlights the importance of balancing security with usability, such as leveraging single sign-on (SSO) and adaptive authentication.

Keeping Up with Regulatory Changes

Compliance requirements are constantly evolving. Gartner advises maintaining flexibility in IAM policies and investing in automation to quickly adapt access controls in response to new regulations.

The Future Outlook of Gartner Identity and Access Management

As digital ecosystems become more complex and threats more sophisticated, Gartner identity and access management insights will continue to be invaluable. Emerging technologies like artificial intelligence, machine learning, and blockchain are poised to reshape IAM capabilities. Gartner is already tracking how AI-driven behavioral analytics can enhance threat detection and how decentralized identity models might empower users with greater control over their data.

Ultimately, organizations that stay informed through Gartner’s IAM research and proactively evolve their identity and access management strategies will be better positioned to protect sensitive assets, comply with regulations, and support seamless digital experiences. The journey toward a more secure digital future is ongoing, and Gartner’s identity and access management guidance remains a trusted compass along the way.

Frequently Asked Questions

What is Gartner's definition of Identity and Access Management (IAM)?

Gartner defines Identity and Access Management (IAM) as a framework of policies and technologies that ensures the right individuals access the right resources at the right times for the right reasons.

Why is IAM important according to Gartner?

Gartner emphasizes IAM's importance in reducing security risks, ensuring compliance, improving user experience, and enabling digital transformation by managing user identities and access privileges effectively.

What are the key components of IAM highlighted by Gartner?

Gartner identifies key IAM components such as identity governance, access management, privileged access management, and identity lifecycle management as essential for comprehensive security.

How does Gartner suggest organizations approach IAM implementation?

Gartner suggests a phased approach focusing first on critical assets, incorporating automation, and aligning IAM strategy with business goals to improve security and operational efficiency.

What trends in IAM are currently emphasized by Gartner?

Gartner highlights trends like passwordless authentication, AI-driven identity analytics, decentralized identity models, and cloud-native IAM solutions as shaping the future of IAM.

How does Gartner evaluate IAM vendors?

Gartner evaluates IAM vendors based on their ability to execute and completeness of vision, considering factors like technology innovation, integration capabilities, scalability, and customer experience.

What role does IAM play in Zero Trust according to Gartner?

Gartner states IAM is foundational to Zero Trust security models by continuously verifying user identities and enforcing least-privilege access controls across all resources.

How is AI impacting IAM solutions as per Gartner's

analysis?

Gartner notes AI enhances IAM by enabling adaptive authentication, anomaly detection, and predictive access management, improving both security and user convenience.

What challenges in IAM does Gartner identify for enterprises?

Gartner identifies challenges including managing hybrid environments, balancing security with user experience, addressing regulatory compliance, and integrating legacy systems within modern IAM frameworks.

Additional Resources

Gartner Identity and Access Management: A Comprehensive Review of Industry Insights and Trends

gartner identity and access management has become a pivotal reference point for organizations aiming to navigate the complex landscape of digital security. As cyber threats evolve and regulatory demands intensify, enterprises increasingly rely on identity and access management (IAM) solutions to safeguard sensitive data and ensure compliance. Gartner, a leading research and advisory company, provides in-depth analysis and market evaluations that guide IT decision-makers in selecting and implementing effective IAM strategies.

Understanding Gartner’s perspective on identity and access management offers valuable insights into the current state and future trajectory of this critical security discipline. This article delves into Gartner’s key findings, market trends, and best practices related to IAM, highlighting how enterprises can leverage these insights to strengthen their security posture.

What is Gartner Identity and Access Management?

At its core, Gartner’s identity and access management research revolves around helping organizations manage digital identities and control user access to resources across various environments—on-premises, cloud, and hybrid. Gartner evaluates IAM technologies and vendors based on criteria such as functionality, scalability, user experience, integration capabilities, and security features.

The Gartner Magic Quadrant for Identity Governance and Administration (IGA) and Access Management are particularly influential reports. They assess vendors’ completeness of vision and ability to execute, helping businesses identify solutions that align with their unique operational requirements.

Defining Key IAM Components According to Gartner

Gartner categorizes IAM into several fundamental components:

- **Identity Governance and Administration (IGA):** Focuses on user identity lifecycle management, access requests, role management, and compliance.
- **Access Management:** Encompasses authentication, authorization, single sign-on (SSO), and adaptive access controls.
- **Privileged Access Management (PAM):** Deals with securing and monitoring privileged accounts to prevent insider threats.
- **Customer Identity and Access Management (CIAM):** Tailors IAM for customer-facing applications, emphasizing user experience and privacy.

These categories underscore the breadth of IAM as a discipline and the specialized solutions that Gartner evaluates.

Key Trends Highlighted by Gartner in Identity and Access Management

Gartner's latest research identifies several trends shaping the IAM market and influencing enterprise adoption:

Cloud-First IAM Strategies

One of the most prominent trends is the migration from traditional on-premises IAM to cloud-based solutions. Gartner emphasizes that cloud IAM platforms offer scalability, faster deployment, and improved integration with SaaS applications. Enterprises are adopting hybrid IAM models that blend on-premises control with cloud agility.

However, Gartner also warns about challenges such as data residency, vendor lock-in, and the need for unified policy enforcement across diverse environments. Organizations must carefully evaluate cloud IAM offerings to ensure alignment with security policies and compliance requirements.

Zero Trust and Adaptive Access

Gartner strongly advocates for a zero-trust approach to IAM, where trust is never implicit, and access decisions are continuously evaluated based on context. Adaptive access mechanisms, such as risk-based authentication and behavioral analytics, are gaining traction. These technologies dynamically adjust authentication requirements based on user behavior, device health, and environmental factors, reducing the risk of unauthorized access.

This shift reflects a broader security paradigm where identity becomes the new perimeter, critical in a world of remote work and distributed networks.

Increased Focus on Identity Governance

With regulatory pressures mounting, Gartner notes that identity governance is rising in importance. Organizations are investing in automated access certification, segregation of duties enforcement, and detailed audit trails. Effective governance reduces the risk of privilege abuse and ensures compliance with standards like GDPR, HIPAA, and SOX.

Gartner’s analysis highlights vendors that excel in providing comprehensive governance capabilities alongside access management features.

Evaluating IAM Vendors: Gartner’s Magic Quadrant Insights

The Gartner Magic Quadrant reports are instrumental in benchmarking IAM vendors. In their latest assessments, Gartner categorizes providers into Leaders, Challengers, Visionaries, and Niche Players, based on their completeness of vision and ability to execute.

Leaders in Identity Governance and Administration

Leaders typically demonstrate:

- Robust, scalable platforms capable of handling complex enterprise environments
- Strong integration ecosystems with cloud and on-premises applications
- Advanced automation and analytics for identity lifecycle management
- Global support and compliance readiness

These vendors often provide unified suites encompassing IGA, access management, and privileged access capabilities, facilitating streamlined deployments.

Access Management Leaders

In access management, Leaders distinguish themselves by offering:

- Flexible authentication methods including biometrics, multi-factor authentication (MFA), and passwordless options
- Seamless user experience via single sign-on across diverse platforms
- Adaptive and context-aware access controls aligned with zero trust principles
- Scalable architectures suitable for millions of identities

Gartner stresses that selecting a vendor from the Leaders quadrant often reduces implementation risk but advises organizations to assess fit based on specific business needs.

Challenges and Considerations in Implementing Gartner-Recommended IAM Solutions

While Gartner identity and access management guidance is invaluable, enterprises must navigate several challenges:

Complexity and Integration

IAM solutions, especially those recommended by Gartner, often come with significant complexity due to the need to integrate with a wide array of legacy systems and cloud services. Organizations must allocate adequate resources for planning, customization, and ongoing management.

User Experience vs. Security Balance

A recurring tension exists between maintaining strong security controls and providing a frictionless user experience. Gartner recommends leveraging adaptive access and risk-based authentication to strike this balance effectively, yet implementation complexity can be a hurdle.

Cost and Total Cost of Ownership (TCO)

Leading IAM platforms may involve substantial upfront and operational expenses. Gartner advises organizations to consider not only licensing costs but also integration, training, and maintenance to fully understand TCO.

Regulatory Compliance Alignment

Ensuring that the IAM solution supports compliance reporting and auditing is essential. Gartner’s governance-focused recommendations aid this, but enterprises must customize policies and workflows to meet industry-specific standards.

The Future of Identity and Access Management According to Gartner

Gartner forecasts continued innovation in IAM, driven by emerging technologies and shifting enterprise requirements:

- **Artificial Intelligence and Machine Learning:** Enhanced detection of anomalous behavior and predictive risk scoring.

- **Decentralized Identity:** Growing interest in blockchain-based identity models that give users more control over personal data.
- **Passwordless Authentication:** Wider adoption to improve security and user convenience.
- **Integration with Security Operations:** Tighter coupling of IAM with Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) tools.

Gartner identity and access management research indicates that organizations embracing these trends will be better positioned to protect digital assets while enabling business agility.

Organizations seeking to navigate the evolving IAM landscape benefit significantly from Gartner’s analytical frameworks and vendor evaluations. By aligning with industry best practices and leveraging leading solutions, businesses can enhance security, streamline operations, and adapt to the dynamic threat environment with confidence.

Gartner Identity And Access Management

Find other PDF articles:
https://old.rga.ca/archive-th-021/files?dataid=DuW42-4387&title=surgical-tech-study-guide-free.pdf

gartner identity and access management: AWS Certified Identity and Access Management (IAM) Cybellium, Welcome to the forefront of knowledge with Cybellium, your trusted partner in mastering the cutting-edge fields of IT, Artificial Intelligence, Cyber Security, Business, Economics and Science. Designed for professionals, students, and enthusiasts alike, our comprehensive books empower you to stay ahead in a rapidly evolving digital world. * Expert Insights: Our books provide deep, actionable insights that bridge the gap between theory and practical application. * Up-to-Date Content: Stay current with the latest advancements, trends, and best practices in IT, Al, Cybersecurity, Business, Economics and Science. Each guide is regularly updated to reflect the newest developments and challenges. * Comprehensive Coverage: Whether you're a beginner or an advanced learner, Cybellium books cover a wide range of topics, from foundational principles to specialized knowledge, tailored to your level of expertise. Become part of a global network of learners and professionals who trust Cybellium to guide their educational journey. www.cybellium.com

gartner identity and access management: Enterprise Identity Management Denis Royer, 2013-03-12 The introduction of Enterprise Identity Management Systems (EIdMS) in organizations even beyond the purely technological level is a costly and challenging endeavor. However, for decision makers it seems difficult to fully understand the impacts and opportunities arising from the introduction of EIdMS. This book explores the relevant aspects for an ex-ante evaluation of EIdMS. Therefore it examines this domain by employing a qualitative expert interview study to better understand the nature of EIdMS, as they are situated between security and productive IT systems.

To this regard, the focus is put on the general nature of EIdMS projects and the constructs being relevant for analyzing such projects in the decision support phase. Based on the derived constructs and thematic topics from the interviews, an explanatory model for EIdMS introductions is derived and iteratively improved and evaluated. Finally, a possible application use-case for the creation of adequate decision support tools is presented.

gartner identity and access management: *Digital Identity and Access Management: Technologies and Frameworks* Sharman, Raj, Das Smith, Sanjukta, Gupta, Manish, 2011-12-31 This book explores important and emerging advancements in digital identity and access management systems, providing innovative answers to an assortment of problems as system managers are faced with major organizational, economic and market changes--Provided by publisher.

gartner identity and access management: *Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities* Ng, Alex Chi Keung, 2018-01-26 Due to the proliferation of distributed mobile technologies and heavy usage of social media, identity and access management has become a very challenging area. Businesses are facing new demands in implementing solutions, however, there is a lack of information and direction. Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities is a critical scholarly resource that explores management of an organization’s identities, credentials, and attributes which assures the identity of a user in an extensible manner set for identity and access administration. Featuring coverage on a broad range of topics, such as biometric application programming interfaces, telecommunication security, and role-based access control, this book is geared towards academicians, practitioners, and researchers seeking current research on identity and access management.

gartner identity and access management: *Handbook of Research on Big Data Storage and Visualization Techniques* Segall, Richard S., Cook, Jeffrey S., 2018-01-05 The digital age has presented an exponential growth in the amount of data available to individuals looking to draw conclusions based on given or collected information across industries. Challenges associated with the analysis, security, sharing, storage, and visualization of large and complex data sets continue to plague data scientists and analysts alike as traditional data processing applications struggle to adequately manage big data. The Handbook of Research on Big Data Storage and Visualization Techniques is a critical scholarly resource that explores big data analytics and technologies and their role in developing a broad understanding of issues pertaining to the use of big data in multidisciplinary fields. Featuring coverage on a broad range of topics, such as architecture patterns, programing systems, and computational energy, this publication is geared towards professionals, researchers, and students seeking current research and application topics on the subject.

gartner identity and access management: Microsoft Certified Exam guide - Security, Compliance, and Identity Fundamentals (SC-900) Cybellium, Unlock Your Path to Success with the Ultimate SC-900 Exam Guide! Are you ready to embark on a journey towards becoming a Microsoft Certified: Security, Compliance, and Identity Fundamentals professional? Look no further! This comprehensive guide, meticulously crafted by experts in the field, is your key to mastering the SC-900 exam and elevating your career in the dynamic world of cybersecurity and compliance. Why This Book? In an era of increasing cyber threats and evolving compliance regulations, Microsoft's SC-900 certification has become a critical milestone for IT professionals looking to establish their expertise in security, compliance, and identity fundamentals. This book is designed to be your trusted companion, providing you with in-depth knowledge and hands-on skills that will not only help you pass the SC-900 exam with flying colors but also excel in your cybersecurity career. What's Inside? · Comprehensive Coverage: Delve into the core concepts of security, compliance, and identity management with a clear and concise approach. We break down complex topics into easy-to-understand chapters, ensuring you grasp every essential detail. · Real-World Scenarios: Gain practical insights into real-world cybersecurity challenges and compliance scenarios. Learn how to apply your knowledge to solve common issues and secure your organization's digital assets effectively. · Hands-On Labs: Put your skills to the test with hands-on labs and exercises. Practice what you've learned in a safe and controlled environment, building confidence and competence. · Exam Preparation: We've got you covered with extensive exam preparation materials. Access practice questions, mock tests, and exam tips to boost your confidence and ensure you're fully prepared for the SC-900 exam. · Expert Guidance: Benefit from the experience and expertise of our authors, who have a proven track record in the cybersecurity and compliance domains. Their insights and guidance will be invaluable as you navigate the complexities of this field. · Career Advancement: Beyond passing the exam, this book equips you with skills that are highly sought after by organizations worldwide. Open doors to new career opportunities and command a higher salary with your SC-900 certification. Who Is This Book For? · IT Professionals: Whether you're just starting your career in IT or seeking to enhance your existing skills, this book is your gateway to success. · Security Enthusiasts: If you have a passion for cybersecurity and aspire to become a certified expert, this guide will help you achieve your goals. · Compliance Officers: Gain a deeper understanding of compliance regulations and how they relate to cybersecurity, making you an indispensable asset to your organization. · Students: Students pursuing degrees in IT or related fields will find this book a valuable resource for building a strong foundation in security, compliance, and identity fundamentals. Take Your First Step Towards Excellence! The SC-900 certification is a testament to your dedication to securing digital assets and ensuring compliance within your organization. Microsoft Certified Exam Guide - Security, Compliance, and Identity Fundamentals (SC-900) is your roadmap to achieving this prestigious certification and unlocking a world of opportunities. Don't wait any longer! Dive into the world of cybersecurity and compliance with confidence. Your future as a certified expert begins here. Get ready to transform your career and make a lasting impact in the ever-evolving landscape of IT security and compliance. © 2023 Cybellium Ltd. All rights reserved. www.cybellium.com

gartner identity and access management: *Cybersecurity First Principles: A Reboot of Strategy and Tactics* Rick Howard, 2023-04-19 The first expert discussion of the foundations of cybersecurity In Cybersecurity First Principles, Rick Howard, the Chief Security Officer, Chief Analyst, and Senior fellow at The Cyberwire, challenges the conventional wisdom of current cybersecurity best practices, strategy, and tactics and makes the case that the profession needs to get back to first principles. The author convincingly lays out the arguments for the absolute cybersecurity first principle and then discusses the strategies and tactics required to achieve it. In the book, you'll explore: Infosec history from the 1960s until the early 2020s and why it has largely failed What the infosec community should be trying to achieve instead The arguments for the absolute and atomic cybersecurity first principle The strategies and tactics to adopt that will have the greatest impact in pursuing the ultimate first principle Case studies through a first principle lens of the 2015 OPM hack, the 2016 DNC Hack, the 2019 Colonial Pipeline hack, and the Netflix Chaos Monkey resilience program A top to bottom explanation of how to calculate cyber risk for two different kinds of companies This book is perfect for cybersecurity professionals at all levels: business executives and senior security professionals, mid-level practitioner veterans, newbies coming out of school as well as career-changers seeking better career opportunities, teachers, and students.

gartner identity and access management: Modernizing Enterprise IT Audit Governance and Management Practices Gupta, Manish, Sharman, Raj, 2023-10-26 Information technology auditing examines an organization's IT infrastructure, applications, data use, and management policies, procedures, and operational processes against established standards or policies. Modernizing Enterprise IT Audit Governance and Management Practices provides a guide for internal auditors and students to understand the audit context and its place in the broader information security agenda. The book focuses on technology auditing capabilities, risk management, and technology assurance to strike a balance between theory and practice. This book covers modern assurance products and services for emerging technology environments, such as Dev-Ops, Cloud applications, Artificial intelligence, cybersecurity, blockchain, and electronic payment systems. It examines the impact of the pandemic on IT Audit transformation, outlines common IT audit risks, procedures, and involvement in major IT audit areas, and provides up-to-date audit concepts, tools, techniques, and references. This book offers valuable research papers and practice articles on managing risks related to evolving technologies that impact individuals and organizations from an assurance perspective. The inclusive view of technology auditing explores how to conduct auditing in various contexts and the role of emergent technologies in auditing. The book is designed to be used by practitioners, academicians, and students alike in fields of technology risk management, including cybersecurity, audit, and technology, across different roles.

gartner identity and access management: *Mastering IAM* Cybellium, In today's interconnected digital landscape, effective Identity and Access Management (IAM) is vital for organizations to secure their systems, protect sensitive data, and enable seamless collaboration. In Mastering IAM, acclaimed author Kris Hermans provides a comprehensive guide that demystifies the complexities of IAM, empowering readers to establish robust identity management practices and optimize access controls. With years of experience in the cybersecurity field, Hermans understands the critical role IAM plays in ensuring the confidentiality, integrity, and availability of digital resources. In this book, he shares his expertise, providing a practical roadmap for implementing and managing IAM solutions that align with business goals and industry best practices. Inside Mastering IAM, you will: 1. Explore the IAM landscape: Gain a deep understanding of the core concepts, components, and frameworks that form the foundation of IAM. From authentication and authorization to identity governance and federation, master the essential building blocks of a successful IAM strategy. 2. Design and implement IAM solutions: Learn how to design an IAM architecture tailored to your organization's needs, considering factors such as scalability, compliance, and user experience. Follow step-by-step guidelines for deploying IAM solutions, including user provisioning, access controls, single sign-on (SSO), and multi-factor authentication (MFA). 3. Enhance security and compliance: Discover strategies for mitigating security risks and ensuring compliance with relevant regulations. Explore identity lifecycle management, privileged access management (PAM), and security incident response to safeguard against threats and unauthorized access. 4. Leverage IAM for business efficiency: Uncover how IAM can streamline business processes, improve productivity, and enhance user experiences. Explore topics such as self-service portals, role-based access control (RBAC), and integration with other systems to optimize IAM functionality. 5. Address emerging challenges: Stay up to date with the latest trends and emerging technologies shaping the IAM landscape. Learn about cloud-based IAM solutions, IoT device management, and the impact of artificial intelligence and machine learning in enhancing IAM capabilities. With real-world examples, practical tips, and insightful case studies, Mastering IAM equips readers with the knowledge and skills needed to effectively implement and manage IAM solutions. Whether you are an IAM professional, IT manager, or security practitioner, this book will guide you toward harnessing the full potential of IAM to protect your organization's assets and drive business success. Don't let identity and access management be a barrier to productivity and security. Unleash the power of IAM with Kris Hermans as your trusted guide.

gartner identity and access management: Information Systems Security Sushil Jajoda, Chandan Mazumdar, 2015-12-16 This book constitutes the refereed proceedings of the 11th International Conference on Information Systems Security, ICISS 2015, held in Kolkata, India, in December 2015. The 24 revised full papers and 8 short papers presented together with 4 invited papers were carefully reviewed and selected from 133 submissions. The papers address the following topics: access control; attacks and mitigation; cloud security; crypto systems and protocols; information flow control; sensor networks and cognitive radio; and watermarking and steganography.

gartner identity and access management: Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications Management Association, Information Resources, 2020-03-06 Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.

gartner identity and access management: Handbook of Research on Enterprise Systems Gupta, Jatinder N. D., Sharma, Sushil, Rashid, Mohammad A., 2009-01-31 Addresses the field of enterprise systems, covering progressive technologies, leading theories, and advanced applications.

gartner identity and access management: Information Technology Risk Management and Compliance in Modern Organizations Gupta, Manish, Sharman, Raj, Walp, John, Mulgund, Pavankumar, 2017-06-19 This title is an IGI Global Core Reference for 2019 as it is one of the best-selling reference books within the Computer Science and IT subject area since 2017, providing the latest research on information management and information technology governance. This publication provides real-world solutions on identifying, assessing, and managing risks to IT systems, infrastructure, and processes making it an ideal publication for IT professionals, scholars, researchers, and academicians. Information Technology Risk Management and Compliance in Modern Organizations is a pivotal reference source featuring the latest scholarly research on the need for an effective chain of information management and clear principles of information technology governance. Including extensive coverage on a broad range of topics such as compliance programs, data leak prevention, and security architecture, this book is ideally designed for IT professionals, scholars, researchers, and academicians seeking current research on risk management and compliance.

gartner identity and access management: Cybersecurity Audun Jøsang, 2024-11-29 This book gives a complete introduction to cybersecurity and its many subdomains. It’s unique by covering both technical and governance aspects of cybersecurity and is easy to read with 150 full color figures. There are also exercises and study cases at the end of each chapter, with additional material on the book's website. The numerous high-profile cyberattacks being reported in the press clearly show that cyberthreats cause serious business risks. For this reason, cybersecurity has become a critical concern for global politics, national security, organizations as well for individual citizens. While cybersecurity has traditionally been a technological discipline, the field has grown so large and complex that proper governance of cybersecurity is needed. The primary audience for this book is advanced level students in computer science focusing on cybersecurity and cyber risk governance. The digital transformation of society also makes cybersecurity relevant in many other disciplines, hence this book is a useful resource for other disciplines, such as law, business management and political science. Additionally, this book is for anyone in the private or public sector, who wants to acquire or update their knowledge about cybersecurity both from a technological and governance perspective.

gartner identity and access management: *Cloud Penetration Testing* Kim Crawley, 2023-11-24 Get to grips with cloud exploits, learn the fundamentals of cloud security, and secure your organization's network by pentesting AWS, Azure, and GCP effectively Key Features Discover how enterprises use AWS, Azure, and GCP as well as the applications and services unique to each platform Understand the key principles of successful pentesting and its application to cloud networks, DevOps, and containerized networks (Docker and Kubernetes) Get acquainted with the penetration testing tools and security measures specific to each platform Purchase of the print or

Kindle book includes a free PDF eBook Book DescriptionWith AWS, Azure, and GCP gaining prominence, understanding their unique features, ecosystems, and penetration testing protocols has become an indispensable skill, which is precisely what this pentesting guide for cloud platforms will help you achieve. As you navigate through the chapters, you'll explore the intricacies of cloud security testing and gain valuable insights into how pentesters evaluate cloud environments effectively. In addition to its coverage of these cloud platforms, the book also guides you through modern methodologies for testing containerization technologies such as Docker and Kubernetes, which are fast becoming staples in the cloud ecosystem. Additionally, it places extended focus on penetration testing AWS, Azure, and GCP through serverless applications and specialized tools. These sections will equip you with the tactics and tools necessary to exploit vulnerabilities specific to serverless architecture, thus providing a more rounded skill set. By the end of this cloud security book, you'll not only have a comprehensive understanding of the standard approaches to cloud penetration testing but will also be proficient in identifying and mitigating vulnerabilities that are unique to cloud environments.What you will learn Familiarize yourself with the evolution of cloud networks Navigate and secure complex environments that use more than one cloud service Conduct vulnerability assessments to identify weak points in cloud configurations Secure your cloud infrastructure by learning about common cyber attack techniques Explore various strategies to successfully counter complex cloud attacks Delve into the most common AWS, Azure, and GCP services and their applications for businesses Understand the collaboration between red teamers, cloud administrators, and other stakeholders for cloud pentesting Who this book is for This book is for aspiring Penetration Testers, and the Penetration Testers seeking specialized skills for leading cloud platforms—AWS, Azure, and GCP. Those working in defensive security roles will also find this book useful to extend their cloud security skills.

gartner identity and access management: Campus Technology , 2007-10

gartner identity and access management: AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense Alauthman, Mohammad, Almomani, Ammar, 2025-04-23 AI-driven security systems and intelligent threat response using autonomous cyber defense represent the cutting edge of cybersecurity technology. As cyber threats become more sophisticated, traditional defense mechanisms struggle to keep up with the scale and speed of attacks. AI-powered security systems utilize machine learning, pattern recognition, and data analysis to detect vulnerabilities, predict breaches, and respond to threats. These systems can learn from emerging threats, adapting to new attack methods and autonomously executing countermeasures without human intervention. By using advanced algorithms to recognize anomalies and mitigate risks, autonomous cyber defense offers a proactive solution to protect sensitive data and networks, ensuring faster responses to cyber incidents. AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense delves into the cutting-edge integration of autonomous systems in cybersecurity, emphasizing AI-driven threat detection, response, and system resilience. It bridges the gap between traditional cybersecurity methods and emerging autonomous defense systems, presenting in-depth coverage of AI-driven security mechanisms, automated threat responses, and intelligent defense strategies. This book covers topics such as cybersecurity, infrastructure, and defense systems, and is a useful resource for engineers, security professionals, business owners, academicians, researchers, and computer scientists.

gartner identity and access management: *Integrating a Usable Security Protocol into User Authentication Services Design Process* Christina Braz, Ahmed Seffah, Bilal Naqvi, 2018-11-08 There is an intrinsic conflict between creating secure systems and usable systems. But usability and security can be made synergistic by providing requirements and design tools with specific usable security principles earlier in the requirements and design phase. In certain situations, it is possible to increase usability and security by revisiting design decisions made in the past; in others, to align security and usability by changing the regulatory environment in which the computers operate. This book addresses creation of a usable security protocol for user authentication as a natural outcome of the requirements and design phase of the authentication method development life cycle.

gartner identity and access management: *Access to Online Resources* Kristina Botyriute, 2018-03-13 This book is published open access under a CC BY 4.0 licence.The book offers a concise guide for librarians, helping them understand the challenges, processes and technologies involved in managing access to online resources. After an introduction the book presents cases of general authentication and authorisation. It helps readers understand web based authentication and provides the fundamentals of IP address recognition in an easy to understand manner. A special chapter is dedicated to Security Assertion Markup Language (SAML), followed by an overview of the key concepts of OpenID Connect. The book concludes with basic troubleshooting guidelines and recommendations for further assistance. Librarians will benefit from this quick and easy read, which demystifies the technologies used, features real-life scenarios, and explains how to competently employ authentication and access management.

gartner identity and access management: Inventive Approaches for Technology Integration and Information Resources Management Khosrow-Pour, Mehdi, 2014-06-30 Today's management world continually relies on technological efficiency to function and perform at a high standard. As technology becomes a greater part in many fields, understanding and managing this factor is integral for organizations. Inventive Approaches for Technology Integration and Information Resources Management provides an overview and analysis of knowledge management in sustainability, emergency preparedness, and IT, among other fields integral to the modern technological era. By providing a foundation for innovative practices in using technology and information resources, this publication is essential for practitioners and professionals, as well as undergraduate/graduate students and academicians.

Related to gartner identity and access management

Gartner是一个什么样的机构？ **-** 知乎 Gartner,Inc.（纽约证券交易所：IT）是全球领先的 信息技术研究和顾问公司，也是 标准普尔500指数 包含的上市公司之一。Gartner为企业领导者提供必不可少的见解、建议和工具，以帮助他

Gartner是什么机构？国内有哪些公司入围过？ **-** 知乎 Gartner Group公司成立于1979年，它是第一家信息技术研究和分析的公司。它为有需要的技术用户来提供专门的服务。

Gartner魔力象限为什么会受到重视？ **-** 知乎 最近，Gartner发布了2021年度的RPA行业魔力象限，引起了科技界的关注，那么这个有着“科技界的奥斯卡”之名的报告为什么会如此受到重视？一、Gartner公司与魔力象限 1979年，Gartner

Gartner 称预计 **2026** 年超过 **80%** 的企业将使用生成式 **AI** 应用，透 Gartner分析师在10月20日的媒体交流活动表示，到2026年，Gartner预测超过80%的企业将使用生成式AI的API或

为什么 **Gartner** 等分析机构都在强调“全栈超融合软件”？ 作为首次发布的全栈超融合软件市场报告，Gartner 还分析了 Nutanix、VMware、Microsoft、SmartX、深信服等代表厂商。其中，SmartX 在 IDC《跟踪报告》中，以 21.9 % 的市场份额

什么网站可以下载免费行业报告？ **-** 知乎 经济、财经、上市公司报告 1、巨潮资讯网 cninfo.com.cn/new/index 巨潮资讯网是深圳证券交易所法定信息披露平台，由深交所全资子公司深圳证券信息有限公司运营。页面简单干净、数据齐

为人熟知的世界权威市场数据调查机构都有哪些？ **-** 知乎 擅长领域：为医药健康产业提供专业信息和战略咨询服务，是制药和保健行业全球领先的市场情报资源提供商。主要业务范围为市场信息调查、向医药保健行业的合作伙伴发布调查数据和商业

Gartner最新发布的**2025**年中国数据安全平台市场指南，提到不少 Gartner最新发布的2025年中国数据安全平台市场指南，提到不少数据安全厂商，有合作过的吗？这些代表性厂商的产品名字都叫数据安全平台，数据安全管理平台，有什么区别呢？

如何获取**Gartner**报告，付费账号怎么申请，年费多少？ **-** 知乎 如何获取Gartner报告，付费账号怎么申请，年费多少？一直想参考一些咨询报告，很多都收费，Gartner需要账号，但没有发现注册或申请的地方 显示全部 关注者 11 被浏览

IDC研究方向，报告与**Gartner** 的主要区别是什么？ **-** 知乎 IDC和Gartner都是全球权威的IT 咨询机构，服务对象覆盖各行各业的IT用户和厂商。就我所在的企业级存储领域来说，两者都会就市场、数据、技术进行研究。但IDC在市场数据方面比较有优

Gartner是一个什么样的机构？ **-** 知乎 Gartner,Inc.（纽约证券交易所：IT）是全球领先的 信息技术研究和顾问公司，也是 标准普尔500指数 包含的上市公司之一。Gartner为企业领导者提供必不可少的见解、建议和工具，以帮助他

Gartner是什么机构？国内有哪些公司入围过？ **-** 知乎 Gartner Group公司成立于1979年，它是第一家信息技术研究和分析的公司。它为有需要的技术用户来提供专门的服务。

Gartner魔力象限为什么会受到重视？ **-** 知乎 最近，Gartner发布了2021年度的RPA行业魔力象限，引起了科技界的关注，那么这个有着“科技界的奥斯卡”之名的报告为什么会如此受到重视？一、Gartner公司与魔力象限 1979年，Gartner

Gartner 称预计 **2026** 年超过 **80%** 的企业将使用生成式 **AI** 应用，透 Gartner分析师在10月20日的媒体交流活动表示，到2026年，Gartner预测超过80%的企业将使用生成式AI的API或

为什么 Gartner 等分析机构都在强调"全栈超融合软件"？ 作为首次发布的全栈超融合软件市场报告，Gartner 还分析了 Nutanix、VMware、Microsoft、SmartX、深信服等代表厂商。其中，SmartX 在 IDC《跟踪报告》中，以 21.9 % 的市场份额

什么网站可以下载免费行业报告？ - 知乎 经济、财经、上市公司报告 1、巨潮资讯网 cninfo.com.cn/new/index 巨潮资讯网是深圳证券交易所法定信息披露平台，由深交所全资子公司深圳证券信息有限公司运营。页面简单干净、数据

为人熟知的世界权威市场数据调查机构都有哪些？ - 知乎 擅长领域：为医药健康产业提供专业信息和战略咨询服务，是制药和保健行业全球领先的市场情报资源提供商。主要业务范围为市场信息调查、向医药保健行业的合作伙伴发布调查数据和商

Gartner最新发布的2025年中国数据安全平台市场指南，提到不少 Gartner最新发布的2025年中国数据安全平台市场指南，提到不少数据安全厂商，有合作过的吗？这些代表性厂商的产品名字都叫数据安全平台，数据安全管理平台，有什么区别呢？

如何获取Gartner报告，付费账号怎么申请，年费多少？ - 知乎 如何获取Gartner报告，付费账号怎么申请，年费多少？一直想参考一些咨询报告，很多都收费，Gartner 需要账号，但没有发现注册或申请的地方 显示全部 关注者 11 被浏览

IDC研究方向，报告与Gartner 的主要区别是什么？ - 知乎 IDC和Gartner都是全球权威的IT 咨询机构，服务对象覆盖各行各业的IT用户和厂商。就我所在的企业级存储领域来说，两者都会就市场、数据、技术进行研究。但IDC在市场数据方面比较有优

Gartner是一个什么样的机构？ - 知乎 Gartner,Inc.（纽约证券交易所：IT）是全球领先的 信息技术研究和顾问公司，也是 标准普尔500指数 包含的上市公司之一。Gartner为企业领导者提供必不可少的见解、建议和工具，以帮助他

Gartner是什么机构？国内有哪些公司入围过？ - 知乎 Gartner Group公司成立于1979年，它是第一家信息技术研究和分析的公司。它为有需要的技术用户来提供专门的服务。

Gartner魔力象限为什么会受到重视？ - 知乎 最近，Gartner发布了2021年度的RPA行业魔力象限，引起了科技界的关注，那么这个有着"科技界的奥斯卡"之名的报告为什么会如此受到重视？一、Gartner公司与魔力象限 1979年，Gartner

Gartner 称预计 2026 年超过 80% 的企业将使用生成式 AI 应用，透 Gartner分析师在10月20日的媒体交流活动表示，到2026年，Gartner预测超过80%的企业将使用生成式AI的API或

为什么 Gartner 等分析机构都在强调"全栈超融合软件"？ 作为首次发布的全栈超融合软件市场报告，Gartner 还分析了 Nutanix、VMware、Microsoft、SmartX、深信服等代表厂商。其中，SmartX 在 IDC《跟踪报告》中，以 21.9 % 的市场份额

什么网站可以下载免费行业报告？ - 知乎 经济、财经、上市公司报告 1、巨潮资讯网 cninfo.com.cn/new/index 巨潮资讯网是深圳证券交易所法定信息披露平台，由深交所全资子公司深圳证券信息有限公司运营。页面简单干净、数据

为人熟知的世界权威市场数据调查机构都有哪些？ - 知乎 擅长领域：为医药健康产业提供专业信息和战略咨询服务，是制药和保健行业全球领先的市场情报资源提供商。主要业务范围为市场信息调查、向医药保健行业的合作伙伴发布调查数据和商

Gartner最新发布的2025年中国数据安全平台市场指南，提到不少 Gartner最新发布的2025年中国数据安全平台市场指南，提到不少数据安全厂商，有合作过的吗？这些代表性厂商的产品名字都叫数据安全平台，数据安全管理平台，有什么区别呢？

如何获取Gartner报告，付费账号怎么申请，年费多少？ - 知乎 如何获取Gartner报告，付费账号怎么申请，年费多少？一直想参考一些咨询报告，很多都收费，Gartner 需要账号，但没有发现注册或申请的地方 显示全部 关注者 11 被浏览

IDC研究方向，报告与Gartner 的主要区别是什么？ - 知乎 IDC和Gartner都是全球权威的IT 咨询机构，服务对象覆盖各行各业的IT用户和厂商。就我所在的企业级存储领域来说，两者都会就市场、数据、技术进行研究。但IDC在市场数据方面比较有优

Related to gartner identity and access management

Okta Named a Leader in 2024 Gartner® Magic Quadrant™ for Access Management for Eighth Consecutive Year (Business Wire9mon) SAN FRANCISCO--(BUSINESS WIRE)--Okta, Inc. (NASDAQ:OKTA), the leading independent Identity partner, today announced that it has been recognized as a Leader in the 2024 Gartner Magic Quadrant for

Okta Named a Leader in 2024 Gartner® Magic Quadrant™ for Access Management for Eighth Consecutive Year (Business Wire9mon) SAN FRANCISCO--(BUSINESS WIRE)--Okta, Inc. (NASDAQ:OKTA), the leading independent Identity partner, today announced that it has been recognized as a Leader in the 2024 Gartner Magic Quadrant for

Gartner Names Microsoft, Okta Among Access Management Leaders (SDxCentral2y) Gartner identified Okta, Microsoft, Ping Identity, ForgeRock, and CyberArk as access management market leaders in its recent Magic Quadrant report. The analysis firm defines access management as

Gartner Names Microsoft, Okta Among Access Management Leaders (SDxCentral2y) Gartner identified Okta, Microsoft, Ping Identity, ForgeRock, and CyberArk as access management market leaders in its recent Magic Quadrant report. The analysis firm defines access management as

Gartner: Businesses struggling with ID management (ZDNet18y) Despite broader recognition of the need for securing access to applications and other IT resources, enterprises are still

struggling to come to terms with the issues involved with identity and access

Gartner: Businesses struggling with ID management (ZDNet18y) Despite broader recognition of the need for securing access to applications and other IT resources, enterprises are still struggling to come to terms with the issues involved with identity and access

Ping Identity Named as a Leader in 2024 Gartner® Magic Quadrant™ for Access Management (FOX31 Denver9mon) DENVER, Dec. 5, 2024 /PRNewswire/ -- Ping Identity, a leader in securing digital identities for the world's largest enterprises, announced that it was named as a Leader in the 2024 Gartner Magic

Ping Identity Named as a Leader in 2024 Gartner® Magic Quadrant™ for Access Management (FOX31 Denver9mon) DENVER, Dec. 5, 2024 /PRNewswire/ -- Ping Identity, a leader in securing digital identities for the world's largest enterprises, announced that it was named as a Leader in the 2024 Gartner Magic

Enterprises still grappling with access management: Gartner (ZDNet18y) Despite broader recognition of the need for securing access to applications and other IT resources, enterprises are still struggling to come to terms with the issues involved with identity and access

Enterprises still grappling with access management: Gartner (ZDNet18y) Despite broader recognition of the need for securing access to applications and other IT resources, enterprises are still struggling to come to terms with the issues involved with identity and access

Identity management top security priority in Gartner survey (Network World15y) “The No.1 priority is now identity and access management,” says Gartner research director Vic Wheatman, noting the analysis is based on a close look at what IT security professionals at 308 companies

Identity management top security priority in Gartner survey (Network World15y) “The No.1 priority is now identity and access management,” says Gartner research director Vic Wheatman, noting the analysis is based on a close look at what IT security professionals at 308 companies

Wave to Showcase Virtual Smart Card Solution at Gartner's Identity and Access Management Summit Nov. 18-20 (Yahoo UK & Ireland11y) LEE, MA--(Marketwired -) - Wave Systems Corp. (NASDAQ: WAVX) will demonstrate its comprehensive solution for activating and managing virtual smart cards for Windows 7, 8 and 8.1 at the

Wave to Showcase Virtual Smart Card Solution at Gartner's Identity and Access Management Summit Nov. 18-20 (Yahoo UK & Ireland11y) LEE, MA--(Marketwired -) - Wave Systems Corp. (NASDAQ: WAVX) will demonstrate its comprehensive solution for activating and managing virtual smart cards for Windows 7, 8 and 8.1 at the

ForgeRock Named a Leader In 2022 Gartner® Magic Quadrant for Access Management for Third Consecutive Year (Business Wire2y) SAN FRANCISCO--(BUSINESS WIRE)--ForgeRock ® (NYSE: FORG), a global digital identity leader, today announced it has been positioned by Gartner as a Leader in the 2022 Gartner Magic Quadrant Leader in

ForgeRock Named a Leader In 2022 Gartner® Magic Quadrant for Access Management for Third Consecutive Year (Business Wire2y) SAN FRANCISCO--(BUSINESS WIRE)--ForgeRock ® (NYSE: FORG), a global digital identity leader, today announced it has been positioned by Gartner as a Leader in the 2022 Gartner Magic Quadrant Leader in

Back to Home: https://old.rga.ca